Feb 14 Agenda item, Anti-Spoofing Provisions of the RAY BAUM'S Act

Tony Rutkowski

Fri 2/8/2019 6:42 AM

To: ajit.pai@fcc.gov <ajit.pai@fcc.gov>; rachael.bender@fcc.gov <rachael.bender@fcc.gov>; ajit.pai@fcc.gov <ajit.pai@fcc.gov>; rachael.bender@fcc.gov <rachael.bender@fcc.gov>; Mike.O'Rielly@fcc.gov <Mike.O'Rielly@fcc.gov>; erin.mcgrath@fcc.gov <erin.mcgrath@fcc.gov>; brendan.carr@fcc.gov <brendan.carr@fcc.gov>; evan.swarztrauber@fcc.gov <evan.swarztrauber@fcc.gov>; jessica.rosenworcel@fcc.gov <jessica.rosenworcel@fcc.gov>; umair.javed@fcc.gov <umair.javed@fcc.gov>; geoffrey.starks@fcc.gov <geoffrey.starks@fcc.gov>; daudeline.meme@fcc.gov <daudeline.meme@fcc.gov>;

Cc: Paul Najarian <NajarianPB@state.gov>; Eric Burger <eric.burger@fcc.gov>;

1 attachments (95 KB)

T17-SG02-C-0167!!MSW-E.docx;

The Chairman and Commissioners should be aware that most of the actions called for in the Act and the Commission's proposed implementation are before the 19-28 February, Geneva, meeting of ITU-T Study Group 2, in the form of a draft Rec. M.rtafm, "Requirements for Telecom anti-Fraud Management in the TMN." See attached contribution from the Recommendation editor.

Study Group 2 has global jurisdiction over the use of telephony services and especially the use of telephone numbers as they are allocated and managed pursuant to ITU-T Rec. E.164. It is therefore an essential venue for implementation of Sec. 503 of Ray Baum's Act.

The Commission should consider support for the Recommendation and involvement in the meeting via the State Dept by appropriate staff.

respectfully,
Anthony M. Rutkowski, EVP for Regulatory and Standards

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG2-C167

STUDY GROUP 2

Original: English

Question(s): 5/2 Geneva, 19-28 February 2019

CONTRIBUTION

Source: China Telecommunications Corporation

Title: The contribution on modifying M.rtafm document.

Purpose: Proposal

Contact: LING Ying
China Telecommunication
China
Tel: +86 21 28970016
Fax: +86 21 58754013
E-mail: lingying@sttri.com.cn

Keywords: Telecom anti-Fraud Management; TMN;

Abstract: This contribution proposes some modification in M.rtafm document based on the document T17-SG02-180704-TD-GEN-0439!!MSW-E.

1. Discussion

This contribution proposes some modification in M.rtafm based on the comments from last meeting in Geneva.

2. Proposals

This contribution proposed some modifications in the document as follows:

1) Adding the new definitions in Chapter 3.2;

2) Modifying the text in Chapter 6.3;

3) Modifying the text in Chapter 7;

4) Adding “8.1.5 Fraud detection management function” and “8.2.4 Fraud mitigation management function” in Chapter 8;

5) Modifying the text in Chapter 9.1;

6) Adding the content of Appendix A.

Draft ITU-T Recommendation M.rtafm

Requirements for Telecom anti-Fraud Management in the TMN

1 Scope

This draft Recommendation describes the requirements for Telecom anti-Fraud Management in the TMN, the functional framework for combating telecom fraud management and the functional description.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.156] ITU-T Recommendation E.156 (2006), *Guidelines for ITU-T action on reported misuse of E.164 number resources*.

[ITU-T E.156 – Suppl. 1] ITU-T Recommendation E.156 – Supplement 1 (2007), *Guidelines for ITU-T action on reported misuse of E.164 number resources. Supplement 1: Best practice guide on countering misuse of E.164 number resources*

[ITU-T E.156 – Suppl. 2] ITU-T Recommendation E.156 – Supplement 1 (2007), *Guidelines for ITU-T action on reported misuse of E.164 number resources. Supplement 2: Possible actions to counter misuse*

[ITU-T M.3010] ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*

[WTSA RESOLUTION 61] WTSA-12 – Resolution 61(2012), *Countering and combating misappropriation and misuse of international telecommunication numbering resources*

3 Definitions

3.1 Terms defined elsewhere

3.1.1 **Fraud:** Fraud is use of numbers in the manner for which they were prescribed, but in a manner intended to generate revenue. The use of a number in the manner for which it was allocated but for the purpose of generating cash at the expense of the customer and/or operators. [ITU-T E.156 – Suppl. 1]

TBD

Editor's note:

- The terms involved in this recommendation should be in accordance with E.156, Supplement 1 and Supplement 2. The changed text will be proposed based on contributions received in the future.

- The fraud calls should be clarified from two aspects as following table.

  - The fraud scenarios should be described.

- It's necessary to describe whether the number resources are misused and how the number resources are used.

Misuse of E.164 number resources	Fraud scenarios
Using an assigned numbering resource. - Some calls are initiated by web dialers using applications to originate calls with false calling party numbers (CPN). These calls are spoofing calls.	**Case 1:** The spoofing calls are often very short. These short calls are generated to consumers with the purpose of leaving a missed call notification on phones display in order to prompt the called party users to call back.
Using an unassigned numbing resource. - In many cases, VoIP technologies have been used, and somewhere in the route not assigned numbering resources have been inserted or reassigned.	**Case 2:** Fraud calls are often use of numbers in manner for which they were prescribed, but in a manner intended to generate revenue or in a malicious manner (such as harassing, threatening, obscene, fraud manner and so on).

- The more fraud scenarios will be described as the appendix of this recommendation based on the contributions received in the future.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **nuisance call:** refers to the unsolicited, annoying telephone call, such as one originating from a telemarketer, robotcaller, or prankster or one that is obscene, harassing, misdialed, or senseless.

3.2.2 **phishing:** refers to the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in a communication. The attacker sends spam emails, SMSes and voice calls aimed at getting banking details of a target.

3.2.3 **telecom anti-fraud management:** is the development, execution and supervision of plans, policies, programs and practices that detect and mitigate telecom fraud activities.

NOTE--Taking full advantage of telecom network operation data, to detect the possible fraud in time and to make the appropriate treatment to mitigate lost revenue due to fraud by means of telecom network management functionalities (including signalling monitoring, data analysis, alarm monitoring, and configuration management).

Contributor's note:

The definition of telecom anti-fraud management had been modified considering the comment from SCV-TD91.

3.2.4 **telecom fraud:** refers to the use of telecom service (telephones, cell phones, computers etc.) to commit the fraud. Victims in telecom fraud include telecom consumers, called party users and communication service providers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CLI	Calling Line Identity
CPN	Calling Party Number

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is not recommended**" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of telecom anti-fraud management in the TMN

6.1 Telecom fraud statements

Telecom fraud refers to the fraudulent activity through the means of communication (such as targeted spear-phishing e-mails or SMSes, spoofing calls or nuisance calls and so on). These fraud activities increasingly impact on telecom consumers, called party users.

The misuse of numbers and numbering plans might form the basis by which a fraud is perpetrated, but the misuse itself might not constitute actual fraud. Telecom fraud is use of numbers in the manner for which they were prescribed, but in a manner intended to generate revenue. Telecom fraud occurs with numbering misuse, including global numbering resources, international numbering resources, national numbering resources, local numbering resources, advertisement emails, SMSes or rogue dialling and so on. [ITU-T E.156 – Suppl. 1]

Telecom fraud behaviours always have the following features:

- Abandoned calls: The calls always end before they are answered by the called party user, which is commonly known as a "sound" phone, to get the consumer to call back to the instigate calls with short stopping. This kind of call occupies a large amount of network resources, which affects the communication quality of users. To induce the user to dial back and not wait the called party user answering, they could, for example, broadcast advertising. Calls to the instigate numbers incurring expensive call charges and exploiting settlement dates to receive payment from operators prior to the call origination costs being settled.
- Abnormal calling party number: Most fraudulent calls use false calling party numbers. Some of calling party numbers entirely or partly fake user's real number, such as numbers of police, government departments, banks, operators, relatives, friends and other types of customer misleading numbers. Some of calling party numbers are not in conformity with international or national numbering plan, such as unsigned country code, unsigned national destination code, ultra-long or ultra-short length.
- The high frequency of the same calling number: Some calling number making call frequency is too high. The same calling number in unit time makes a large number of outgoing calls. These numbers are suspected and worthy of attention excluding some service numbers.

- Continuous called number: If a calling party number initiates call more than 5~10 continuous called party numbers, it usually can be judged as a call where numbers are being misappropriated or misused.
- Very short interval calls: Dialer devices may be used to misappropriate or misuse numbers. The call interval is always very short. Sometimes the calls are made through the relay. It even could generates a large number of concurrent calls.
- The high frequency of the same called number: Some phone numbers are called very frequently due to fraud calls. It influences the experience of these called party users. In these cases, the calling numbers which have received a certain amount of complaints from called party users can be judged as misappropriated or misused.

Fraud can emerge from premium rate services, telephone number misuse and mobile. [ITU-T E.156 – Suppl. 1]

Based on the above description, victims of telecom fraud include telecom customers, called party users, telecom operators. Losses caused by telecom fraud as following:

- For telecom customer, the loss is the expensive payment for the premium rate services.
- For called party user, the losses are the financial loss based on fraudulent information, and the time loss due to fraud calls.
- For telecom operator, the losses are the bills that cannot be settled, and the waste of network resources.

6.2 Telecom anti-fraud management function requirement

When it comes to comprehensively counteracting telecom fraud, telecom anti-fraud system requires three-capabilities to address this problem: monitoring, detection, and mitigation. These capabilities include: Steps to be taken in order to find suspicious activity from various event data in the first place; actions to detect fraud earlier in the process when it happens; and actions to take to mitigate fraud if suspicious activities are detected.

Telecom anti-fraud includes three procedures as follows:

- Firstly, it is to detect or discover the fraud calls based on the signalling analysis or the call feature analysis. It is necessary to establish the telecom anti-fraud number library including whitelist, blacklist and suspected graylist. It needs to share the number information with the other security departments.
- Secondly, it is to monitor, identify and confirm the suspected calling party number (CPN) in the telecom anti-fraud number library. The numbers identified as fraud callers are added to the blacklist. The CPN in the white list should be confirmed; the CPN in the graylist should be monitored.
- Thirdly, it is to deal with the different types of calling party numbers. The CPN in the blacklist should be blocked. The system blocks domestic and international calls, although most unwanted calls come from abroad. It’s necessary to remind the called party users by voice and SMS messages about the suspected CPN. The telecom anti-fraud number library should be continuously updated.

The purpose of telecom anti-fraud management is to manage the number lists or the related information which generated in the process of fraud detection and mitigation. Telecom anti-fraud management could be divided into two parts: fraud detection management and fraud mitigation management.

- Fraud detection management: refers to detect fraudulent activities based on the telecom network data analysis or the customer complaint informant.

- Fraud mitigation management: refers to the management of prevention in advance or remedial measures after the event.

7 Functional framework for telecom anti-fraud management

The functional framework for telecom anti-fraud management which is shown in Figure7-1 includes the following parts:

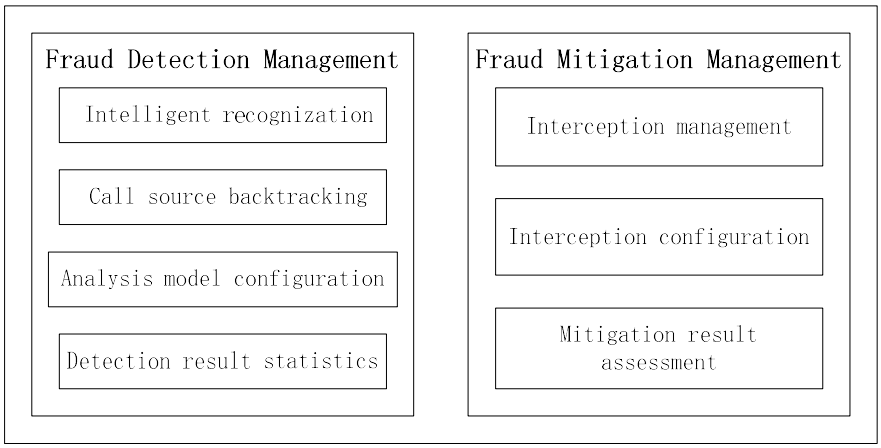

Figure 7-1 – Functional framework for telecom anti-fraud management

- Fraud Detection Management

Fraud detection management module carries out intelligent recognition of signalling data and network routing data to analyze whether there are fraudulent call features. It also performs call source backtracking after the fraudulent calls are detected. It establishes different analysis models for different fraudulent call features. It also analyses and statistics the results of detection.

In order to block nuisance calls and spoofing calls (described in Appendix A), it's necessary to verify the calling party's authorization to use a telephone number (essentially as the international calling line identity (CLI)).

- Fraud Mitigation Management

Fraud mitigation management module is responsible for querying, tagging, generating new lists, removing the repetition, and the other management of the fraudulent calls that need to be intercepted. It also performs interception configuration based on the list of fraudulent calls, including source interception, calling party interception, called party interception and the other configuration rules. It also analyses and statistics the result of interception implementation.

The object of telecom fraud detection is the signalling data and network routing data that existed in the telecom network. The numbers of fraud detection or fraud mitigation should be stored in the number list.

In the nuisance calls scenarios, the nuisance calls should be blocked by the terminating carrier.

8 The functions of each part in the framework

The functions of each component are further explained in this clause.

8.1 Fraud Detection Management

The fraudulent calls could be analyzed based on the CDR (Call Detail Record). The CDR contains the call generate time, response time, called number, network entity (such as signalling point code, IP address) and the related information on user behavior and so on. Through the analysis of these information and combined with the characteristics of fraud call behavior, the fraud call can be detected and intercepted.

The fraudulent calls could also be analyzed by application servers of telecom operator or third-party service provider, based on network capability exposure function. The network could provide the call event information (e.g. calling number, called number, call event, timestamp of call event) to the application servers of telecom operator or third-party service provider, by the means of network capability exposure. Through the analysis of the information provided, combined with the historical data about calling numbers which have received customer complaints, the fraud call can be detected and intercepted.

8.1.1 Intelligent recognization function

Intelligent recognization function requirements include:

- Detect the abnormal calling party number: If the calling party number fakes user's real number, the intelligent recognization module should be able to detect the different incoming source from the normal number. If the calling party number is not in conformity with international or national numbering plan, the intelligent recognization module should be able to detect the suspicious number with unsigned country code, unsigned national destination code, ultra-long or ultra-short length. Service of customer complaint about the abnormal calling party number could be supported as a major way to extend the pool of the abnormal calling party number. The pool of abnormal calling party number should be shared among the different operators.
- Detect the high frequency of the same calling party number: The intelligent recognization module should count the frequency of call initiated by the calling party. If the frequency of one call exceeds a specific value (e.g. 300 times per hour), it could be regarded as a fraudulent call.
- Detect the continuous of the called party number: The intelligent recognization module should count the number of continuous called parties which are called by the same calling party. If the number of continuous called parties exceeds a specific value (e.g. 10 continuous called parties which are called by the same calling party), it could be regarded as a fraudulent call.
- Detect the very short interval calls: The intelligent recognization module should detect the interval between the calls. If the interval is very short, even the calls initiated at the same time, it could be regarded as a fraudulent call.

8.1.2 Call source backtracking function

Call source backtracking function requirements include:

- Trace the source of the fraudulent calls: The call source backtracking module should be able to trace the Interprovincial or international regional.
- Analyze the source direction ratio: The call source backtracking module should count the international, provincial or inter network call ratios.

8.1.3 Detection model configuration function

The fraudulent calls could be divided into three types including: the abnormal calls (e.g. the calling party number comes from the abnormal number pool), the malicious calls (e.g. the malicious group call and the ultrashort harassment call) and the false imitation calls (e.g. the call initiated by the fake calling party imitated the customer service number).

Detection model configuration function requirements include:

- Configure the specific analyse models: According to the feature of the fraudulent calls, the analysis model configuration module should configure different types of analysis models. The analysis models include the calling party number analysis model for the international call with high frequency, the discreteness analysis model for the called party number, the normative analysis model for the calling party number, the calling party analysis model for the call completion abnormity ratio and so on.

8.1.4 Detection result statistics function

Detection result statistics function requirements include:

- Suspicious number list management: The analysis and statistics module should be able to set the hazard level for the calling party number of the fraudulent calls. It should dynamically update,

query or rank the fraudulent call list.

- Source analysis: The analysis and statistics module should analyze the source office direction, the source office and so on.
- Region analysis: The analysis and statistics module should analyze the suspicious interprovincial or international call flow or office and so on.
- Depth analysis dimension: The analysis and statistics module should analyze the number of calls, call distribution, call flow direction, the timely rate of problem discovery and fraud mitigation, the effective rate of fraud mitigation and so on.
- Monitoring dimension: The analysis and statistics module should monitor the warning, fraudulent call upward trend and so on.

8.1.5 Fraud detection management function

In the process of telecom anti-fraud detection, fraud detection management function requirements include:

- Fraud call number library management function: It should continuously update fraud detection number library (e.g. number adding, number withdrawal and so on). It should share the number information in the telecom anti-fraud management system. It also should interface with other security departments.
- Statistical function of call monitoring results: The statistical analysis objects include the call frequency, call duration time and the called party number range of the suspected fraud call.
- Called party user notification management function: The called party user should be reminded about the fraud calling party numbers. It should manage the notification list.

8.2 Fraud Mitigation Management

When the fraud call is detected, the telecom fraud mitigation management provides the functions to identify parties to fraudulent calls (e.g. set up a suspected codes list to monitor them), and to reduce revenue losses caused by such calls in a proportionate manner whenever appropriate (e.g., as soon as customers complaints are produced or worse, some suspected fraud call should be screened).

8.2.1 Interception management function

Interception management function requirements include:

- Suspicious number list management: The interception management module should be able to manage the fraudulent call list that need to be intercepted, including querying, tagging, generating new lists, removing the repetition and so on. It should be able to tag the unprocessed numbers, the numbers in monitoring, the numbers not in monitoring, the numbers in the interception, the numbers not in the interception, white list and so on. It should be able to query the numbers of different areas and states.

8.2.2 Interception configuration function

Interception configuration function requirements include:

- Interception configuration: The interception configuration module should be able to configure the capacity of equipment to intercept the call source, calling party, called party and so on.

8.2.3 Mitigation result assessment function

Mitigation result assessment function requirements include:

- Interception statistics: The mitigation result statistics module should be able to update the statistics on the success rate of interception, the distribution of intercepting implementation and so on.

8.2.4 Fraud mitigation management function

In the process of telecom anti-fraud detection, fraud mitigation management function requirements include:

- Fraud mitigation number library management function: It should continuously update fraud mitigation number library (e.g. number adding, number withdrawal and so on). It should share

the number information in the telecom anti-fraud management system.
- Statistical function fraud mitigation results: This function assesses the fraud call blocking result (e.g. the ratio of fraud calls).

Editor's note:
- More ways on Fraud Mitigation will be described in future, including interception, as well as the cooperation on Fraud Mitigation will be enhanced among operators, society and individuals.

9 The function sets for telecom anti-fraud management

9.1 Fraud Detection Management

Fraud Detection Management provides functions to detect telecom fraud calls, such as abnormal call, malicious call, false imitation call and so on.
Fraud Detection Management includes the following function set groups:

- Detection of Telecom Fraud Call.
- Tracking of Telecom Fraud Call.
- Analyse Pattern Setting.
- Fraud Call Detection Reporting.

9.1.1 Detection of Telecom Fraud Call

Detection of Telecom Fraud Call provides functions to detect telecom fraud calls based on the call features such as the abnormal calling party number, the call with malicious behavior, or false imitation call and so on.
Detection of Telecom Fraud Call includes the following function sets:

- Administration of abnormal calling party number function set.
- Investigation of the call with malicious behavior function set.
- Administration of false imitation call function set.

9.1.1.1 Administration of abnormal calling party number list function set

This set provides access to information about the numbering plans of normal calling party number and the list of abnormal calling party number with unassigned country code (CC), unassigned national destination code (NDC), ultra-long or ultra-short number length and so on.
Numbers identified as fraud calls by the operator's experts are added to an operator-maintained blacklist and calls from such number are sent to the user's junk voicemail.
The fraud calls from specific categories (such as withheld or international) should be sent straight to the user's junk voicemail.
The blacklist is continuously updated to block phone numbers. The blocked numbers come from dynamic lists of known spam callers. The list includes the phone numbers of call centres that use spurious sales pitches, call at inconvenient times (before 8 am or after 8 pm and at weekends) or do not comply with a national code.
The blacklist includes respecting directory listings marked with an asterisk to stop nuisance calls and display of the caller's own number.
The list also contains numbers blocked personally by users. These numbers are not added to the black list immediately. A number of criteria are also checked before the relevant number is placed on the general blacklist.

9.1.1.2 Investigation of the call with malicious behavior function set

This set supports the analysis of the call with malicious behavior such as the high frequency of the same calling party number, the continuous of the called party number, the very short interval calls

and so on. This set also supports the investigation of suspected malicious call based on the complaint from the victims.
If a user gets an unwanted call he/she can quickly add it to their personal blacklist. All future calls from that number will be sent to the user's junk voicemail.

9.1.1.3 Administration of false imitation call list function set
This set provides access to a list of the false imitation calls which have the imitated calling party number, caller's name or company and so no.

9.1.2 Tracking of Telecom Fraud Call
Tracking of Telecom Fraud Call provides functions to find where the telecom fraud call comes from.
Tracking of Telecom Fraud Call includes the following function sets:

- Analysis of the regional area of fraud call initiated function set.
- Analysis of the fraud call direction function set.

9.1.2.1 Analysis of the regional distribution area of fraud call initiated function set
This set supports the generation of reports to analyse the regional distribution area of the fraud calls which are initiated.

9.1.2.2 Analysis of the fraud call direction function set
This set supports the generation of reports to analyse the regional distribution area of the victims.

9.1.3 Analysis Pattern Setting
Analysis Pattern Setting provides functions to configure the specific fraud call analysis patterns according to the features of fraud call.
Analysis Pattern Setting includes the following function set:

- Analysis pattern setting function set.

9.1.3.1 Analysis pattern setting function set

This set supports to set different call analysis pattern in the network to detect the specific fraud call.

9.1.4 Fraud Call Detection Reporting
Fraud Call Detection Reporting provides functions to receive, store and summarize fraud call detection information.
Fraud Call Detection Reporting includes the following function sets:

- Administration of suspected fraud calls function set.
- Analysis of fraud calls detection function set.

9.1.4.1 Administration of suspected fraud calls function set
This set provides access to information about the suspected fraud calls. The fraud calls should be set different hazard level. The fraud call list could be dynamically updated, queried or ranked.

9.1.4.2 Analysis of fraud calls detection function set
This set supports the generation of reports to analyse the source office of fraud call which is initiated, the suspected interprovincial or international call flow of fraud call. It also supports to analyze the count of fraud calls, call distribution, call flow direction and the timeliness rate of problem discovery and so on. It also supports to monitor the fraud call upward trend and alarm surveillance.

9.2 Fraud Mitigation Management
Fraud Mitigation Management provides functions to mitigate telecom fraud calls.
Fraud Mitigation Management includes the following function set groups:

- Administration of Fraud Mitigation List.
- Fraud Mitigation Configuration

- Fraud Mitigation Assessment.

9.2.1 Administration of Fraud Mitigation List

Administration of Fraud Mitigation List provides functions to access to information about the suspected fraud calls which are need to be mitigated.
Administration of Fraud Mitigation List includes the following function set:

- Administration of fraud mitigation list function set.

9.2.1.1 Administration of fraud mitigation list function set.

This set provides access to information about the fraud mitigation list. The fraud mitigation list with the mitigation processing state could be queried, updated, removed and tagged. The fraud mitigation list could be queried by areas, call sources and so on.

9.2.2 Fraud Mitigation Configuration

Fraud Mitigation Configuration provides functions to configure the equipments in network to intercept the suspected fraud call.

Fraud Mitigation Configuration includes the following function set:

- Fraud mitigation configuration function set.

9.2.2.1 Fraud mitigation configuration function set

This set supports the network equipment configuration to intercept the fraud call based on the call features.

9.2.3 Fraud Mitigation Assessment

Fraud Mitigation Assessment provides functions to assess the fraud mitigation result.
Fraud Mitigation Assessment includes the following function set:

- Fraud mitigation assessment function set.

9.2.3.1 Fraud mitigation assessment function set

This set provides access to the assessment summary of the fraud mitigation result. It includes the evaluation of effect after fraud mitigation (i.e. interception success rate etc.).

Editor's note:

- In the future, we should focus on the proposals of how to use the TMN function to implement the function sets for telecom anti-fraud management.

APPENDIX A

Telecom Fraud Scenarios

The advancement of technological tools such as computers, the internet, and cellular phones has made life easier and more convenient for most people in our society. However some individuals and groups have subverted these telecom devices into tools to defraud numerous unsuspecting victims. It is not uncommon for a scam to originate in a city, country, state, or even a country different from that in which the victim resides.

Telecom fraud can be divided into two types of scenarios as follows.

A.1 Nuisance Calls

Nuisance calls and messages come in a variety of different shapes and sizes and can be inconvenient and annoying to the users. Nuisance calls have the following scenarios:

- Silent calls: The phone rang but there was no one on the other end of the line.
- Abandoned calls: The users were played an information message from a company saying it had tried to call them but none of its operators were free to take the call.
- Unsolicited telesales calls
- Recorded marketing message calls: A recorded marketing message was played when the users answered the phone.
- Unsolicited marketing faxes: A marketing fax has been sent to users personal/business fax machine.
- Unsolicited marketing texts: Users are received a text marketing a particular product or service.
- Abusive and threatening calls: Malicious, abusive or threatening calls, whether from people who know or from strangers, are a criminal offence.

The nuisance calls always have malicious purposes, such as voice mail hacking, robotcalling, phishing or uncivil practices known as false report of an incident to emergency services.

The communications providers should be able to stop nuisance calls getting through to consumers in the first place. The communications providers block problem calls at source based on evidence of fraud. It also enables the telephone number of the person making the call to be displayed to the person receiving the call. This helps the call recipient to make a more informed decision about whether to accept the call, and to report problem calls to regulators and law enforcement agencies more effectively.

A.2 Spoofing Calls

Many phone handsets now could display the calling party number before called party user answer. This feature - known as 'Caller ID' or 'Calling Line Identity' (CLI) - is a handy way of screening the calls that want to answer from the ones that don't want to answer. Nuisance callers and criminals deliberately changing the Caller ID, these calls are a practice known as 'spoofing calls'.

Sometimes there's a good reason for a caller to modify the Caller ID to leave an 0800 number for called party users to call back if they want.

However, with spoofing callers deliberately change the telephone number and/or name relayed as the Caller ID information. They do this to either hide their identity or to try to mimic the number of a real company or person who has nothing to do with the real caller. For example, identity thieves who want to steal sensitive information such as users’ bank account or login details, sometimes use spoofing to pretend they're calling from users’ bank or credit card company.

Calls with spoofed numbers come from all over the world and account for a significant and growing proportion of nuisance calls. Voice over IP (VoIP) technology - the type of technology used to make internet calls - is often used in spoofing.

Spoofing call is the use of rogue web dialers to originate calls on the PSTN or on the Internet with false CPN (Calling Party Number) or CLI (Calling Line Identity). This makes the call appear as though it's being made by someone else and it has become a common form of misuse and misappropriation of numbering resources. It is especially pernicious for operators because they have no way of preventing these spoofing calls with their numbers and they only ever learn of them from other operators or the recipients.

In the current network environment, there appears more and more untrustable devices (including the PABX, call centre and VoIP access system) that interconnect to PLMN/PSTN. As a result, a huge number of phone numbers are leased to anonymous call providers who help fuel phone spam. Noticeably, Caller ID spoofing is particularly effective at defeating static call blockers, thus leading to a variety of scams by avoiding identification. Current mechanisms aimed at avoiding voice scam and ping calls are insufficient from a user's stand point. It's difficult to validate the spoofing calls.

Further, illegal bypass of international calls using Over-The-Top (OTT) telecom applications, including innovative techniques to disguise these practices, has caused significant loss to national revenues and national operators revenues as well as inconveniences to the consumers.

_____